On Sets of Integers Not Containing Long Arithmetic Progressions

Izabella Łaba*
University of British Columbia

Michael T. Lacey†
Georgia Institute of Technology

October 22, 2001

After this paper was completed, we learned that the main result had in fact been proved much earlier by R.A. Rankin ("Sets of integers containing not more than a given number of terms in arithmetical progression", Proc. Roy. Soc. Edinburgh Sect. A 65 (1960/1961), 332–344). Since very few people appear to have been aware of that result, I have decided to leave the present paper on my web page as an expository note, with the above explanation added.

1 The Main Result

Let $r(k, N)$ be the maximal cardinality of a subset A of $\{1, 2, \ldots, N\}$ which does not contain an arithmetic progression of length k. That is, A does not contain a subset of the form $\{x + jy : 0 \leq j < k\}$, where x, y are integers with $y \neq 0$.

Erdös and Turan [3] initiated the study of these quantities in 1936. In particular they conjectured that $r(k, N) = o(N)$ for all k, that is every set of integers of positive asymptotic density contains arbitrarily long arithmetic progressions. In 1953, Roth [8] showed that $r(3, N) = o(N)$. The Erdös–Turan conjecture was verified by Szemerédi [11, 12], a result with a very broad influence. Subsequently, rather different proofs of Szemerédi's theorem were given by Furstenberg [4] and Gowers [5, 6]. Gowers's proof provides, for the first time, upper bounds on $r(k, N)$ given by a bounded tower of exponentials. An intriguing question of Erdös asks if $r(3, N) \leq CN/(\log N)^{1+\delta}$ for some positive δ. Bourgain's article [2] contains the best current upper bound of $CN\sqrt{\frac{\log\log N}{\log N}}$ on $r(3, N)$.

*Supported in part by NSERC
†Supported by an NSF grant, DMS–9706884.

In this article we are interested in the converse question of finding large subsets of $\{1,\dots,N\}$ which do not contain arithmetic progressions. Behrend, in 1946, [1] (building on earlier work of Salem and Spencer [10]) considered three term arithmetic progressions, and showed that $r(3,N) \geq N \exp(-C\sqrt{\log N})$. The purpose of this paper is to show that if one considers longer arithmetic progressions then Behrend's estimate can be further improved as follows.

Theorem 1 *There is a constant $C > 0$ so that for all $n > k \geq 1$,*

$$r(1+2^k, N) \geq N \exp(-C(\log N)^{1/(k+1)}). \tag{1.1}$$

2 The Proof

Our argument builds upon the methods of Salem and Spencer [10] and of Behrend [1]. It will be convenient to consider the set $I = \mathbf{Z} \cap (-\frac{N-1}{2}, \frac{N-1}{2}]$ instead of $\{1,2,\dots,N\}$. First, we may assume that $N = n^d$ for suitably chosen integers n and d, with n much smaller than N and divisible by a constant c_0 (independent of N, n) to be chosen later. Indeed, at the cost of a slightly larger constant in our theorems we can always increase n to one of these values. Similarly, we shall take fractional powers and logarithms of large integers and tacitly assume that the output is also an integer. In fact the argument requires the integer parts of these quantities, but to minimize notation we do not explicitly invoke the integer part function.

Second, with $N = n^d$, consider the expansion of each $x \in I$ in base n, defined as follows. For any $x \in I$ we define its coordinate vector $v_x = (x_0, \dots, x_{d-1}) \in \mathbf{Z}^d$, where x_i are uniquely determined by the conditions

$$x = \sum_{i=0}^{d-1} x_i n^i, \ -\frac{n-1}{2} < x_i \leq \frac{n-1}{2}. \tag{2.2}$$

Note that, unlike in Behrend's argument, the "digits" x_i are not required to be non-negative. Denote also the "norm" of $x \in I$ as

$$\|x\|^2 = \|v_x\|^2 = \sum_{i=0}^{d-1} x_i^2,$$

with x_i defined by (2.2).

An important observation of Salem and Spencer [10] was that if we only consider the set Q_0 of numbers $x \in \{0,1,\dots,N-1\}$ with digits $0 \leq x_i < cn$, where c is sufficiently small[1],

[1]Salem and Spencer considered expansions with non-negative digits $0 \leq x_i \leq n-1$, in which case it suffices to take $c = 1/2$

then addition of numbers is equivalent to vector addition in the corresponding subset of $\mathbf{Z}^d$, i.e. for any $x, y, z \in Q_0$ we have $x + y = z$ if and only if $v_x + v_y = v_z$. Thus an arithmetic progression $x, x + y, x + 2y, \ldots$ in Q_0 corresponds to vectors $v_x, v_{x+y}, v_{x+2y}, \ldots$ on a straight line in $\mathbf{Z}^d$.

We shall rely on variants of this observation. More precisely, we define

$$Q = \{x \in \mathbf{Z} : \ x = \sum_{i=0}^{d-1} x_i n^i, \ -q \leq x_i \leq q\}, \tag{2.3}$$

where $q = n/c_0$ and c_0 is a large constant independent of N, n to be chosen later. We will also denote for $r \in \mathbf{Z}$:

$$rQ = \{x \in \mathbf{Z} : \ x = \sum_{i=0}^{d-1} x_i n^i, \ -rq \leq x_i \leq rq\}.$$

Then linear combinations of numbers in rQ with small enough integer coefficients correspond to linear combinations of their coordinate vectors:

$$v_{\sum a_k x^{(k)}} = \sum a_k v_{x^{(k)}} \text{ if } a_k, r_k \in \mathbf{Z}, \ x^{(k)} \in r_k Q, \ \sum r_k |a_k| < c_0/3. \tag{2.4}$$

Our proof consists of two distinct parts, both similar in spirit to Behrend's argument [1]. The latter relies on the geometrical fact that a straight line can intersect a sphere $\|v_x\|^2 = r$ in $\mathbf{Z}^d$ in at most two points, so that the set $\{x \in Q : \ \|x\|^2 = r\}$ cannot contain a three-term arithmetic progression. One then uses pigeonholing to choose a sphere containing a large number of points in Q.

Our intermediate results can be stated in terms of quantities closely related to those of Erdös and Turan. Namely, define $r_m(k, N)$ to be the maximal cardinality of a subset $A \subset \{0, 1, \ldots, N-1\}$ which does not contain a further subset of the form

$$\Big\{x + \sum_{i=1}^{m} a_i j^i \ : \ 0 \leq j < k - 1\Big\}, \tag{2.5}$$

for any integers x and a_i such that at least one of the a_i is non-zero. (In particular, $r_1(k, N) = r(k, N)$ and $r_m(k, n)$ decreases with m.) Observe that a set of the form (2.5) with $u \geq 2$ may contain less than k distinct integers, as the same summand may arise from more than one value of j. Note further that the a_i need not belong to A. Finally, while this is defined as a property of the initial interval of integers $\{0, \ldots, N-1\}$, it depends only on the length of the interval of integers in question.

The estimates we will need are the following.

Proposition 2 *We have*

$$r_m(2m+1, N) \geq N \exp(-C\sqrt{\log N}), \tag{2.6}$$

where C is an absolute constant depending only on m.

Proposition 3 *Assume that $N = n^d$, and let $k \geq m+1$. Then*

$$r_m(k, N) \geq N \frac{r_{2m}(k, n^2 d)}{c^d\, n^2 d}, \tag{2.7}$$

where the constant $c > 0$ depends only on m and k.

Proposition 2 is proved by essentially repeating Behrend's argument with straight lines replaced by curves of higher order; the main point is that a non-constant polynomial of degree $2m$ can have at most $2m$ roots. Proposition 3 will allow us to carry out the inductive argument. Instead of just one sphere as in Behrend's argument, the set A which provides the lower bound in (2.7) will be a union of concentric spheres of radii $\sqrt{r}$, $r \in R$. We will argue that if A contains a subset $\{x^{(j)}\}$ as in (2.5), then the squared norms $\|x^{(j)}\|^2$ are as in (2.5) with m replaced by $2m$. Proposition 3 will follow upon choosing a set R of cardinality $r_{2m}(k, dn^2)$ which cannot contain such a subset, and optimizing over n and d.

We will use C, c, c_i, etc. to denote absolute constants which may depend on m and may change from line to line but are always independent of N, n, d.

3 Proof of Proposition 2

Our goal in this section is to find a set $R \subset \{0, 1, \ldots, N-1\}$ of large cardinality such that R does not contain all of the integers

$$\sum_{i=0}^{m} a_i j^i : \ j = 0, 1, \ldots, 2m \tag{3.8}$$

for any $a_0, \ldots, a_m \in \mathbf{Z}$ with $a_i \neq 0$ for at least one $i > 0$. We will use the notation of Section 2. In particular, we will replace the set $\{0, 1, \ldots, N-1\}$ by I, and assume that $N = n^d$ for some $1 \ll d \ll N$ and $1 \ll n \ll N$ (eventually we will let $d \sim \sqrt{\log N}$). The set R will be a subset of the set Q defined in (2.3).

Lemma 4 *Suppose that $2m+1$ numbers $x^{(j)}$ in Q satisfy*

$$x^{(j)} = \sum_{i=0}^{m} a_i j^i, \ j = 0, 1, \ldots, 2m, \tag{3.9}$$

for some integers $a_0, \dots, a_m$. Denote by D the Vandermonde determinant $D = D_m = |J_m|$, where $J_m = (j^i)_{i,j=1}^m$. Then there is a constant c, depending only on m, such that

$$Da_i \in cQ, \ \ i = 0, \dots, m. \tag{3.10}$$

Furthermore, if the constant c_0 in the definition of Q was chosen large enough, then we have for any such numbers

$$Dv_{x^{(j)}} = \sum_{i=0}^{m} j^i \, v_{Da_i}, \ \ j = 0, 1, \dots, 2m. \tag{3.11}$$

Proof. We consider the first $m+1$ equations in (3.9) as a system of linear equations with unknowns $a_0, \dots, a_m$. By Cramer's formula, Da_i are linear combinations of $x^{(j)}$ with integer coefficients bounded by a constant depending only on m. This implies (3.10). Now (3.11) follows from (3.10), (3.9) and (2.4). ∎

We are now in a position to run Behrend's argument. Let

$$S_r = \{x \in Q : \ \|x\|^2 = r\},$$

where $\|x\|^2 = \|v_x\|^2 = \sum_{i=0}^d |x_i|^2$. We will prove that no S_r may contain $2m+1$ points as in (3.9). Indeed, suppose to the contrary that $x^{(j)}$, $j = 0, 1, \dots, 2m$, satisfy (3.9) and $\|x^{(j)}\|^2 = r$. By Lemma 4, we have

$$P(j) := \|x^{(j)}\|^2 = \sum_{k=0}^{d-1} \Big(\sum_{i=0}^{m} \frac{(Da_i)_k}{D} j^i \Big)^2.$$

But then $P(j)$ is a polynomial of degree $2m$ in j, equal to r for $j = 0, 1, \dots, 2m$. This is not possible unless $P(j)$ is constant, in which case we must have $(Da_i)_k = 0$ for all $0 \le k \le d-1$ and all $1 \le i \le m$. By Lemma 4 again, it follows that $a_i = 0$ for all $1 \le i \le m$.

Finally, we use a pigeonholing argument to find a set S_r of large cardinality. Following Behrend [1], we set $d = \sqrt{\log N}$ and $n = N^{1/d}$, so that $q = N^{1/d}/1000$. Since Q has cardinality $(2q)^d$ and $Q = \bigcup_{r=0}^{dq^2} S_r$, there is at least one r for which

$$N^{-1} \# S_r \ge (d 500^d q^2)^{-1} \ge C_1 \exp(-C_1 d) N^{-2/d} \ge C_1 \exp\Big(- C_1 \Big(d + \frac{\log N}{d} \Big) \Big).$$

Taking $d = \sqrt{\log N}$ proves the proposition.

4 Proof of Proposition 3

We continue to use the notation of Section 2: we assume that $N = n^d$ with $n, d \ll N$, and define q, Q, v_x, $\|x\|$, D, etc. as before. We also define

$$(x, y) = \sum_{i=0}^{d-1} x_i y_i$$

for $x, y \in \frac{c_0}{3} Q$.

Let $R \subset \{0, 1, \dots, D^2 dq^2 - 1\}$ be a set of cardinality $r_{2m}(k, D^2 dq^2)$ which does not contain all of the integers

$$y^{(j)} = \sum_{i=0}^{2m} a_i j^i, \ \ j = 0, 1, \dots, k-1, \tag{4.12}$$

for any $a_0, \dots, a_{2m} \in \mathbf{Z}$. Observe that any translate $R + s := \{r + s : \ r \in R\}$, $s \in \mathbf{Z}$, of R has the same cardinality as R and cannot contain k integers as in (4.12). Let $X = 2q \sum_{i=0}^{d-1} n^i \in 2Q$ and $S := \{0, 1, \dots, 9D^2 dq^2\}$. For $s \in S$, define

$$A_s = \{x \in Q : \ D^2 \|x - X\|^2 \in R + s\}.$$

We claim that no A_s can contain k integers

$$x^{(j)} = \sum_{i=0}^{m} b_i j^i, \ \ j = 0, 1, \dots, k-1. \tag{4.13}$$

Indeed, suppose to the contrary that A_s does contains such k integers. As in Lemma 4, we prove that

$$D v_{x^{(j)} - X} = \sum_{i=0}^{m} j^i \, v_{Db_i} - D v_X, \ \ j = 0, \dots, k-1,$$

provided that c_0 was chosen large enough. Hence

$$D^2 \|x^{(j)} - X\|^2 = \sum_{k=0}^{d-1} \Big(\sum_{i=0}^{m} j^i (Db_i)_k - 2Dq \Big)^2$$

are as in (4.12). But this is impossible by the choice of R.

A pigeonholing argument shows that there is an A_s with large cardinality. For any $x \in Q$ we have $q \le (X - x)_i \le 3q$ for each i, hence $D^2 dq^2 \le D^2 \|x - X\|^2 \le 9D^2 dq^2$. Hence for any $x \in Q$ and $r \in R$ we have

$$1 \le \|x - X\|^2 - r \le 9D^2 dq^2,$$

and in particular there is a $s \in S$ such that $D^2\|x - X\|^2 = r + s$. It follows that for each $x \in Q$ there are at least $\#R$ values of s such that $x \in A_s$. Hence

$$\sum_{s \in S} \#A_s \geq \#R \cdot \#Q.$$

In particular, there is an $s \in S$ such that

$$\#A_s \geq \frac{\#R \cdot \#Q}{\#S} \geq C \frac{n^d}{1000^d} \cdot \frac{r_m(k, D^2 d n^2)}{D^2 n^2 d},$$

which yields (2.7).

5 Proof of Theorem 1

We will prove that for all $1 \leq k \ll \log N$ and all $1 \leq l \leq k$,

$$r_{2^{k-l}}(1 + 2^k, N) \geq N \exp\,(-c(\log N)^{\frac{1}{l+1}}). \tag{5.14}$$

In particular, taking $l = k$ we obtain (1.1). Here and below, the constants c, c', c'' may depend on m, k, l, but not on N.

The proof of (5.14) is by induction in l. The case $l = 1$ is (2.6). Suppose now that (5.14) holds for l, and set $N = n^d$, $d \sim (\log N)^{1/(l+2)}$. Then by (2.7) we have

$$r_{2^{k-l-1}}(1 + 2^k, N) \geq N \frac{r_{2^{k-l}}(1 + 2^k, n^2 d)}{c^d\, n^2 d} \geq N c^{-d} \exp\,(-c'(\log(n^2 d))^{\frac{1}{l+1}})$$

$$\geq N \exp\,(-c''(\log N)^{\frac{1}{l+2}}),$$

which is (5.14) for $l + 1$.

References

[1] F.A. Behrend, On sets of integers which contain no three terms in arithmetic progression, Proc. Nat. Acad. Sci. 32 (1946), 331-332.

[2] J. Bourgain, On triples in arithmetic progression, Geom. Func. Anal. 9 (1999) 968—984.

[3] P. Erdös and P. Turan, On some sequences of integers, J. London Math. Soc. 11 (1936), 261—264.

[4] H. Furstenberg, Ergodic behaviour of diagonal measures and a theorem of Szemerédi on arithmetic progressions, J. Analyse Math. 31 (1977), 204—256.

[5] W.T. Gowers, A new proof of Szemerédi's theorem for arithmetic progressions of length four, Geom. Func. Anal. 8 (1998), 529—551.

[6] W.T. Gowers, A new proof of Szemerédi's theorem, Geom. Func. Anal. 11 (2001), 465–588.

[7] D.R. Heath-Brown, Integer sets containing no arithmetic progressions, J. London Math. Soc. (2) 35 (1987), 385—394.

[8] K.F. Roth, On certain sets of integers, J. London Math. Soc. 28 (1953), 245—252.

[9] K.F. Roth, Irregularities of sequences relative to arithmetic progressions, IV, Period. Math. Hungar. 2 (1972), 301—326.

[10] R. Salem and D.C. Spencer, On sets of integers which contain no three terms in arithmetic progression, Proc. Nat. Acad. Sci. 32 (1942), 561—563.

[11] E. Szemerédi, On sets of integers containing no four elements in arithmetic progression, Acta Math. Acad. Sci. Hungar. 20 (1969), 89—104.

[12] E. Szemerédi, On sets of integers containing no k elements in arithmetic progression, Acta Arith. 27 (1975), 299—345.

Izabella Łaba
Department of Mathematics
University of British Columbia
Vancouver, B.C. V6T 1Z2, Canada
ilaba@math.ubc.ca
http://www.math.ubc.ca/~ilaba

Michael T. Lacey
School of Mathematics
Georgia Institute of Technology
Atlanta, GA 30332, U.S.A.
lacey@math.gatech.edu
http://www.math.gatech.edu/~lacey